jamf

Guía práctica sobre la telemetría de Apple para terminales

Lo que ve es lo que hay

La visibilidad comienza con la telemetría

¿Alguna vez ha entrado en una habitación completamente oscura? Sin luz, no puede distinguir claramente las formas, como dónde termina la pared y dónde comienza el borde de un mueble. La seguridad de terminales y, por extensión, la conformidad, son muy parecidas a eso. Sin datos de telemetría, no puede proteger lo que no puede ver.

Aunque esto pueda parecer obvio, la incapacidad de capturar datos actuales sobre el estado de los terminales de las flotas de Apple gestionadas representa uno de los mayores desafíos para las organizaciones modernas actuales. Sin duda, un equipo de TI puede averiguar fácilmente cuántos dispositivos macOS, iOS y iPadOS están inscritos, y los equipos de seguridad pueden generar un informe que detalle cuántos dispositivos se actualizaron a la última versión principal de macOS durante un proyecto de migración realizado hace seis meses.

Pero, ¿pueden sus equipos de TI y seguridad validar el estado de conformidad de la flota de Mac y dispositivos móviles en este mismo instante? **Dicho de otro modo, ¿qué tan seguros están sus equipos de los datos con los que trabajan para verificar lo siguiente:**

- ¿Qué procesos se están ejecutando?
- ¿Se ha visto afectada la integridad del sistema?
- ¿Quién realizó esos cambios?
- ¿Los terminales cumplen con los requisitos de conformidad?

Observe la diferencia sutil pero importante entre las palabras *identificar* y *verificar*. Porque, entre esos dos términos, radica la diferencia entre los dispositivos inscritos: aquellos que tienen registros en su solución de gestión de dispositivos móviles (MDM) que solo se actualizan durante los registros programados (identificar). Y los terminales conformes: la supervisión activa recopila y analiza datos de telemetría enriquecidos para ofrecer información en tiempo real sobre el estado de los terminales (verificar).

El primero se basa en el registro más reciente, que, según la programación y los recursos, puede estar desactualizado y suponer un riesgo desconocido para las organizaciones. El segundo se basa en datos de estado actuales para validar la conformidad de los terminales en tiempo real, y ofrece a los auditores pruebas con fecha y hora de la conformidad de los dispositivos.

Para organizaciones de cualquier tamaño, la clave para cerrar la brecha entre identificar y verificar es la telemetría. **En esta guía, no solo destacamos el papel fundamental que desempeña la telemetría en las estrategias modernas de gestión y seguridad, sino que también abordamos lo siguiente:**

- Qué es y qué no es
- Su papel en la generación de información sobre la flota
- Cómo la visibilidad:
  - Habilita operaciones de TI integrales
  - Impulsa los resultados empresariales deseados
  - Aporta valor mediante una mayor alineación
  - Refuerza la postura de seguridad organizacional

Para establecer expectativas: aunque contar con un centro de operaciones de seguridad dedicado, un equipo especializado de analistas o experiencia en inteligencia de amenazas ciertamente ayuda, no son requisitos indispensables. Lo único necesario es comprender lo que ofrece la telemetría, para que los equipos creen procesos proactivos basados en la toma de decisiones en tiempo real y fundamentada en datos, en lugar de depender de procesos reactivos basados en información desactualizada.

Lo que es la telemetría

Si observamos la etimología de la palabra telemetría, veremos que es un compuesto de dos palabras derivadas del griego: tele, que significa "lejano", y metron, que significa "medida". En términos generales, esto se traduce como "medición remota".

En el contexto de la seguridad de terminales, la telemetría es el flujo de mediciones de estado y actividad que un dispositivo reporta sobre sí mismo: qué se ejecutó, qué cambió, quién lo cambió, cuándo y a qué se conectó.

En lo que respecta a los terminales macOS, la telemetría suele incluir lo siguiente:

- **Seguimiento de acceso**: registra quién inició sesión, cuándo y desde dónde, qué recursos solicitó y qué permisos se concedieron o denegaron, como las solicitudes de escalado de privilegios.
- **Ejecución de procesos**: hace seguimiento del inicio de apps, las tareas en segundo plano, los procesos secundarios relacionados y sus interacciones con el kernel y el espacio de usuario.
- **Eventos del sistema:** registran la desviación de la configuración, los aciertos y errores de actualización, las modificaciones de archivos del sistema y los cambios de estado del hardware o software.
- **Actividad de red:** captura detalles de la conexión, como el nivel de cifrado y los tipos de red, la información de IP, los puertos, los protocolos y las apps que transmiten datos.
- **Registros de diagnóstico:** recopilan datos de funcionamiento y rendimiento del sistema, junto con informes de fallos, estados del código y volcados de memoria.

Al analizar la telemetría, es habitual descartar los artefactos individuales por considerarlos insignificantes o fáciles de pasar por alto. Sin embargo, así como una sola pieza de un rompecabezas no dice mucho por sí sola, la imagen completa se revela cuando se combinan todas las piezas. Juntos, ofrecen a los equipos de TI y seguridad un análisis detallado que verifica el estado de los terminales en ese momento específico.

Lo que los equipos hacen con esas mediciones, ya sea la búsqueda de amenazas, la gestión de parches o la validación de la conformidad, es un paso independiente.

Lo que la telemetría no es

Como ocurre con la mayoría de los controles de seguridad en una estrategia de defensa en profundidad, los administradores deben comprender dónde existen las brechas para poder aplicar capas de defensa que las cierren de la forma más eficaz posible. Asimismo, para usar la telemetría de forma eficaz, debe estar tan familiarizado con sus limitaciones como con sus beneficios.

La telemetría no es:

- Vigilancia de la actividad personal o los hábitos de navegación de un usuario.
- Un sustituto de las herramientas que realizan tareas de gestión o procesos de corrección de seguridad.
- Una certificación general de conformidad durante todo el ciclo de vida de un terminal.

Los datos de telemetría son simplemente información recopilada sobre un dispositivo (o toda la flota de dispositivos) que reside en los registros. Sin ninguna acción adicional, la telemetría tiene poca utilidad por sí sola. La telemetría aporta valor cuando las organizaciones la utilizan: primero, al revisarla o transmitirla a su solución de gestión de eventos e información de seguridad (SIEM) para su análisis, y luego, al aplicar ese contexto en la toma de decisiones basada en datos dentro de los procesos de gestión, seguridad y conformidad.

Esta distinción es importante.

Recopilar datos de telemetría sin aplicarlos a las soluciones de MDM y seguridad de terminales es como el bloque único de aluminio que Apple usa para fabricar cada MacBook. El aluminio, por sí solo, no ayuda a los usuarios a realizar tareas relacionadas con el trabajo. Sin embargo, al aplicar el aluminio a sus procesos de fabricación, Apple logra producir un ordenador que permite a los usuarios cumplir con las responsabilidades de su puesto o sus proyectos creativos.

En esta analogía, la telemetría es la materia prima (el aluminio). Solo al aplicarla pueden las organizaciones construir su programa de conformidad con ella, y todo comienza con una visibilidad integral y los patrones que surgen al combinar los puntos de datos individuales.

Cómo funciona la telemetría: de la consulta al conocimiento

Ahora que hemos explicado en qué consiste la telemetría, cambiemos un poco de perspectiva para analizar cómo los datos de telemetría alojados en los terminales transforman la toma de decisiones relacionadas con la postura de seguridad de los dispositivos y de la organización.

Para comprender mejor cómo fluye la telemetría, analicemos más de cerca cada una de las cuatro etapas del flujo de datos:

1 Recopilación

La plataforma macOS genera un flujo de eventos a nivel de sistema que captura todo lo que ocurre en un dispositivo en tiempo real. Estos datos de estado se recopilan a nivel del kernel y desde los sensores de hardware, y registran las métricas de rendimiento supervisadas por la API de seguridad de terminales de Apple.

2 Agregación

Una vez recopilados los datos sin procesar, el siguiente paso es procesar esta información mediante el sistema de registro unificado (ULS). Durante esta fase, los datos capturados se formatean para cumplir con los requisitos de estructura y almacenamiento de cada dispositivo.

3 Procesamiento

Después de que los datos se registran, las herramientas nativas de macOS, como XProtect y MRT, junto con los agentes de seguridad de terceros, acceden al flujo de registros en tiempo real. Estas herramientas leen y analizan el flujo de datos, priorizando los eventos de mayor relevancia para la etapa final.

4 Creación de informes

En esta etapa, los datos de telemetría enriquecidos que se han estructurado y procesado se transmiten a través de protocolos estándar de origen, como los servidores de diagnóstico de Apple para revisar informes de fallos y estadísticas de uso, así como herramientas de análisis de datos de terceros.

Una vez que los datos de telemetría han recorrido todo el proceso, es habitual que los equipos de TI y seguridad revisen los registros de los dispositivos mientras evalúan el estado de los terminales para identificar posibles problemas. Debido a la cantidad de registros que genera un solo dispositivo, multiplicada por la cantidad de dispositivos de toda la flota, se recomienda encarecidamente que las organizaciones envíen este flujo interminable de datos a su solución SIEM, donde se organiza según los niveles de gravedad o las necesidades de conformidad de la organización. En resumen, en lugar de examinar miles de entradas en busca de la proverbial aguja en un pajar, la tecnología se encarga del trabajo pesado al ordenar los eventos más importantes para que se revisen primero.

Según el tamaño y los recursos disponibles de su organización, este es el punto en el que los equipos multifuncionales se basan en los detalles de los datos de telemetría para resolver los problemas detectados.

Por ejemplo, las organizaciones con equipos dedicados de TI y seguridad cada vez se integran más en un solo departamento, y aprovechan sus fortalezas para aplicar una política de conformidad en los terminales a los que les falta un parche crítico. El equipo de seguridad verifica que el hallazgo sea un verdadero positivo, mientras que el equipo de TI se asegura de que los dispositivos no conformes se agrupen correctamente dentro del MDM. Trabajar en conjunto marca el punto de inflexión, en el que estos equipos se aseguran de que la solución de seguridad de terminales realice la corrección automática y de que la conformidad se valide mediante la recopilación de datos de telemetría actualizados.

Para aclarar: comprender cómo la telemetría brinda información a los equipos no requiere memorizar cada protocolo, tipo de datos o llamada a la API involucrados en el proceso subyacente. Se trata de saber cómo viajan los datos a lo largo del flujo y qué les indican a los equipos de TI y seguridad sobre el estado actual de sus dispositivos, destacando el camino más conforme a seguir.

Visibilidad: el resultado que hace posible la telemetría

La telemetría y la visibilidad se diferencian de una manera importante: la telemetría es la entrada y la visibilidad es la salida. A menudo, estos términos se usan indistintamente porque son similares, pero es importante no confundirlos, ya que son lo bastante distintos como para justificar la diferencia.

Una forma sencilla de identificar la diferencia es: causa y efecto. La telemetría revela la "causa" de un problema, como un dispositivo mal configurado. La visibilidad identifica en qué consiste exactamente la mala configuración y qué dispositivos se ven afectados por ella, lo que también se conoce como el "efecto".

Desde una perspectiva operativa, la visibilidad significa que los equipos cuentan con una evaluación actual y precisa de lo que ocurre en toda su flota. También indica un camino concreto para mitigar los problemas detectados. Responde a preguntas como:

- ¿Se observa el comportamiento previsto según la línea base?
- ¿Qué dispositivos están en buen estado?
- ¿Cuáles están en riesgo?
- ¿Existe una amenaza activa?

La telemetría es el conjunto de datos recopilados que hace posible la visibilidad. Se compone de la información recopilada de todos los terminales gestionados de su flota, y ofrece detalles en tiempo real sobre el estado de los dispositivos, como:

- Parches de sistema o seguridad faltantes
- Apps no autorizadas instaladas
- Configuraciones que se han modificado respecto a la línea base

Si bien la telemetría hace posible la visibilidad, no lo hace de forma automática. Las organizaciones pueden supervisar constantemente sus terminales y recopilar grandes cantidades de telemetría, y aun así carecer de visibilidad sobre el estado y la conformidad de su flota.

Telemetría = entrada

Visibilidad = salida

¿Cómo es posible recopilar telemetría, pero carecer de visibilidad?

Telemetría ≠ visibilidad.

La primera activa y alimenta a la segunda, pero solo cuando los datos se revisan, se contextualizan y se convierten en una decisión o acción. Sin la revisión de datos y la toma de decisiones, la telemetría es como un libro que no se lee: simplemente permanece almacenado, lleno de conocimiento extraordinario, sin beneficiar nunca al usuario.

En lugar de pensar en la visibilidad como un interruptor de encendido/apagado, es más preciso verla como un espectro. En un extremo, la visibilidad existe, mientras que en el extremo opuesto, no existe. Con esto en mente, piense en su organización y en qué punto de la escala de visibilidad se encuentra.

Mientras hace eso, analicemos el ejemplo de una empresa situada en dos extremos distintos del espectro de visibilidad:

Sin visibilidad: una organización exige que los dispositivos estén inscritos en el MDM y utiliza un intervalo de registro predeterminado de 12 horas para actualizar los registros de los dispositivos. Este escenario ofrece información limitada sobre el estado de los dispositivos y ninguna visibilidad en tiempo real. Debido al retraso en el registro, en el mejor de los casos, cualquier dato que recopile tendrá al menos 12 horas de antigüedad. Si los dispositivos no realizan un registro programado, la recopilación se repetirá en la siguiente ventana programada, lo que hace que esa información quede aún más desactualizada.

Aunque el MDM es capaz de hacer mucho, no fue diseñado para funcionar como sustituto de una solución de seguridad de terminales. Esto significa que no se recopilan los indicadores de riesgo, como la presencia de malware o la supervisión de comportamientos sospechosos. Además, los procesos de contención no se pueden ejecutar automáticamente, lo que afecta la postura de seguridad debido a la falta de visibilidad.

Visibilidad habilitada: una organización exige que los dispositivos estén inscritos en el MDM, utiliza un intervalo de registro predeterminado de 12 horas para actualizar los registros de los dispositivos, y cuenta con una solución de seguridad de terminales integrada que supervisa los terminales de forma activa. Juntos, ofrecen información integral sobre el estado de los dispositivos y visibilidad en tiempo real. A pesar del retraso en el registro programado del MDM, la supervisión activa significa que el agente de seguridad transmite constantemente datos de telemetría a través del proceso, lo que permite conocer con precisión el estado de cada terminal de la flota en tiempo real.

Con la seguridad de terminales integrada junto con una solución MDM, los comportamientos, las apps y el código riesgosos se supervisan en todo momento, y cuando se detectan, se bloquean automáticamente. Además, también se pueden llevar a cabo procesos como poner en cuarentena los terminales comprometidos y mitigar riesgos, junto con proporcionar a los equipos datos de estado actuales para aplicar la conformidad mediante la gestión basada en políticas o validar la conformidad ante los auditores con evidencia con fecha y hora.

En resumen, la visibilidad es el resultado de usar la telemetría como una auténtica ventaja de seguridad. No se trata de contratar más personal ni de comprar más herramientas, sino de convertir en información la telemetría que ya generan sus dispositivos macOS, iOS/iPadOS. Y usar esa información como base para decisiones y acciones escalables, con la confianza de conocer el estado real de su flota en crecimiento, no lo que podría ser o lo que era hace uno o dos días, la última vez que se revisó.

La detección, la investigación y la respuesta se impulsan gracias a la visibilidad.

La visibilidad no es valiosa solo por la información que brinda a los equipos técnicos en relación con la conformidad y su impacto en la postura de seguridad. Su valor se extiende a las operaciones diarias de los equipos de TI y seguridad, específicamente:

Detección

El equipo de TI utiliza líneas base para definir los procedimientos operativos normales y los niveles de rendimiento, según las mejores prácticas y adaptados a la organización. La telemetría y, por extensión, la visibilidad, brindan a los equipos información sobre el estado de los dispositivos, como si las configuraciones se ajustan a las líneas base o se han desviado de ellas. La visibilidad también hace que resalte el comportamiento anómalo, incluido todo lo que se haya desviado de la línea base. Esto resulta especialmente beneficioso a medida que las flotas crecen, ya que permite detectar anomalías antes en lugar de después. En otras palabras, la visibilidad en tiempo real detecta de forma proactiva los problemas que, de otro modo, podrían permanecer latentes y pasar desapercibidos hasta convertirse en un incidente.

Investigación

Podría decirse que aquí es donde la visibilidad desempeña su papel más importante. En el momento en que se detecta una anomalía, los equipos de seguridad pasan al modo de investigación para validar el problema y luego responder a una gran cantidad de preguntas, como:

- ¿Qué pasó?
- ¿Cuándo ocurrió?
- ¿Por qué ocurrió?
- ¿Qué tan profundo es el impacto?

Para decirlo sin rodeos, sin telemetría, las respuestas a estas y otras preguntas críticas se basarán únicamente en conjeturas, suposiciones y rumores derivados de las declaraciones de los usuarios. Esto no quiere decir que esos relatos sean incorrectos, sino que imponen una carga mayor a los equipos técnicos, que deben corroborarlos. En cambio, la telemetría es evidencia: es la prueba clara que explica lo que ocurrió a lo largo de la cronología de eventos.

Respuesta

La mejor frase para describir la influencia de la visibilidad en esta operación es *"donde la comprensión se convierte en acción"*. Una vez detectado el problema y revisada la evidencia por parte del equipo de seguridad, un proceso de respuesta a incidentes basado en telemetría brinda a los equipos la información necesaria para realizar tareas en un orden repetible que maximice la corrección y limite la exposición:

- Aislar los terminales comprometidos para contener el impacto.
- Priorizar las amenazas según los niveles más altos de gravedad o criticidad.
- Mitigar los riesgos para erradicar las amenazas persistentes.
- Corregir los terminales, restableciendo el rendimiento a la línea base.

> > >

Cómo responder: sin y con visibilidad

Anteriormente en este libro electrónico, destacamos el contraste entre una organización que cuenta con visibilidad y una que no tiene ninguna visibilidad. La diferencia clave radica en aplicar activamente los datos de telemetría recopilados en el primer caso, frente a recopilarlos sin utilizarlos (o depender de datos desactualizados) en el segundo. Si bien ejemplos como este aparecen claramente a lo largo de esta guía, en ningún lugar se ilustra con mayor claridad que cuando los equipos técnicos trabajan bajo presión durante la respuesta a un incidente.

Los siguientes puntos muestran el marcado contraste entre dos equipos (A y B) encargados de responder al mismo incidente: una aplicación vulnerable y no autorizada instalada en un dispositivo proporcionado por la empresa provoca un ataque de ransomware.

Equipo A: sin visibilidad

- **Trabaja con información parcial:** puede ver las apps instaladas, pero no puede verificar el nivel de vulnerabilidad.
- **Reacciona a medida que aparecen los síntomas:** el rendimiento del dispositivo es lento al principio; más tarde, los datos se vuelven inaccesibles.
- **Fuentes de datos no verificables:** la información se presenta desde la perspectiva del usuario afectado y no se puede corroborar.
- **La resolución requiere trabajo adicional:** al no contar con indicadores que lo corroboren, se necesitan más pasos de resolución de problemas para corregir la causa raíz.
- **No escala con la flota:** a medida que crecen las flotas de dispositivos, las cargas de trabajo aumentan exponencialmente, al igual que los factores de riesgo y las ventanas de exposición.

Equipo B: con visibilidad

- **Los datos integrales llenan los vacíos:** observa el mismo incidente desde dentro, con la causa, la secuencia y el efecto claramente definidos.
- **De la detección a la resolución:** corrige el incidente con una comprensión completa de la cronología, sin conjeturas.
- **Actual, precisa y validada:** la información certifica el estado del terminal tanto a los equipos como a los auditores.
- **Revisar los datos con contexto:** la información recopilada incluye indicadores obtenidos del kernel y los sensores, que ofrecen una imagen completa.
- **Ampliar la flota, no la carga de trabajo:** pensando en la escalabilidad, los procesos se ajustan sin aumentar la carga administrativa.

Trabajo más inteligente, no más arduo

La telemetría es un impulsor de la automatización.

Al integrar la gestión de dispositivos móviles, la seguridad de terminales y la gestión de identidades y accesos, los procesos basados en telemetría pueden potenciar las estrategias de gestión y seguridad de dispositivos de formas novedosas que aprovechan la tecnología para encargarse del trabajo pesado en numerosos escenarios, lo que permite a los administradores centrar sus habilidades en ofrecer experiencias mejoradas y alinear mejor las operaciones con los resultados empresariales.

Considere una automatización basada en políticas en la que la seguridad de terminales señala una app vulnerable y activa la corrección mediante su solución MDM. Este proceso sencillo mantiene la postura de seguridad y mitiga el riesgo sin interrumpir al usuario, involucrar al soporte de TI o convertirse en un incidente.

Las organizaciones modernas han visto cómo las tecnologías de IA/AA pueden convertirse en un multiplicador de fuerza para equipos de cualquier tamaño. Los procesos impulsados por IA pueden buscar amenazas sofisticadas en toda la flota a velocidades increíbles. Correlaciona los datos de telemetría recopilados de los terminales, los analiza y los compara en tiempo real con múltiples bases de datos de inteligencia de amenazas de código abierto y cerrado para detectar amenazas desconocidas y alertar a los equipos. Y con opciones de automatización escalables, mantener a una persona involucrada en los incidentes que lo requieran es tan fácil de incorporar a su proceso como los procesos basados en políticas que gestionan por sí solos los problemas menos graves.

Al poder personalizar las soluciones para adaptarlas a las necesidades específicas de su organización, los incidentes se resuelven más rápido y con mejor información, lo que minimiza el riesgo y el esfuerzo manual, a la vez que optimiza la eficiencia y maximiza la eficacia.

La telemetría en contexto: conformidad, operaciones y valor organizacional

Además de los beneficios de búsqueda de amenazas y respuesta a incidentes analizados anteriormente, hay otras dos áreas que merecen la misma importancia en la forma en que las organizaciones piensan sobre la telemetría.

Conformidad

Sectores como la salud, las finanzas y la educación enfrentan un escrutinio normativo cada vez mayor a nivel mundial. Los mandatos federales y regionales exigen que las organizaciones demuestren que los datos se mantienen seguros y que los dispositivos que los procesan permanecen configurados según los requisitos de conformidad.

Vale la pena repetir un punto: las afirmaciones de conformidad deben verificarse. El criterio predeterminado al que recurren la mayoría de los auditores se basa en esta idea: si no puede verificar que un dispositivo era conforme, entonces no lo era. Así de simple.

La telemetría es el ingrediente secreto que hace posible la validación. Como se mencionó anteriormente, la telemetría en sí misma no es más que un conjunto de datos. Sin revisión, contextualización, decisiones o acciones, no hace posible la visibilidad. De igual manera, sin los controles y políticas de seguridad adecuados implementados de antemano, la telemetría no garantiza la conformidad.

Con el contexto aplicado y los controles implementados, la telemetría se convierte en el impulsor de los aspectos que demuestran (o refutan) que funcionan correctamente en el momento de la evaluación. Más allá de las auditorías formales, los datos probatorios (telemetría) son importantes en otros asuntos de conformidad: las operaciones, que analizaremos en la siguiente sección, y los seguros de ciberseguridad. En ese caso específico, las aseguradoras suelen solicitar a las organizaciones que demuestren pruebas de sus prácticas de seguridad antes de que comience o se renueve la cobertura, o cuando una organización presenta un reclamo.

Operaciones

Los mismos datos de telemetría también benefician a las operaciones de TI, como se mostró anteriormente en los ejemplos de detección, investigación y respuesta. Esto ayuda a los equipos de TI y seguridad a llevar a cabo las tareas relacionadas con sus funciones, y además ofrece a los líderes y ejecutivos de TI una vista en tiempo real del estado y la conformidad de la organización, sin necesidad de un proceso independiente, tareas adicionales ni la generación de informes individualizados.

La telemetría es multifacética y, al basar los informes en telemetría en tiempo real, cumple una doble función: resulta operativamente útil para los equipos técnicos en el día a día, y también respalda casos de uso empresarial mediante documentación creíble y respaldada por evidencia sobre los estados de conformidad y las evaluaciones de riesgo, lo que impulsa futuras conversaciones de crecimiento basando la toma de decisiones en datos precisos y actuales.

En pocas palabras: el valor fundamental de la telemetría no cambia según el tamaño del equipo o la estructura organizacional. La telemetría cumple la misma función, ya sea que la revise un solo gerente de TI o un equipo de analistas de seguridad. Merece un alcance más amplio. En lugar de ser algo que "solo usan los equipos de seguridad", la telemetría cumple distintos propósitos según las necesidades de cada usuario.

Evaluación de su postura de telemetría y visibilidad

Comprender la telemetría y la visibilidad a nivel conceptual es útil. Saber cómo ayuda a las organizaciones a conocer su situación actual es aún más útil. Una autoevaluación de su propia situación en materia de telemetría y visibilidad es un excelente punto de partida para las organizaciones, sin necesidad de comprar herramientas nuevas, capacitación especializada ni cambiar la configuración de su conjunto de soluciones actual.

Comience por responder lo siguiente:

1. ¿Su organización conserva los datos de registro de los terminales en el propio dispositivo, o los transmite a una ubicación central (solución SIEM) para su análisis?
2. ¿Su equipo podría determinar con confianza la postura de seguridad actual de cualquier dispositivo de su flota?
3. ¿Pueden reconstruir la cronología de un incidente utilizando evidencia, o deben depender únicamente de la descripción de los hechos que brinda el usuario afectado?
4. ¿Su organización puede generar una verificación de conformidad con fecha y hora para una auditoría, si se solicitara hoy mismo?
5. Cuando se detectan infracciones de conformidad, ¿se corrigen automáticamente o requieren seguimiento manual?

Las respuestas a las preguntas anteriores revelan mucho sobre la postura de seguridad de su organización y, sobre todo, **la capacidad de su equipo para mitigar riesgos de forma proactiva en lugar de responder de forma reactiva** a un incidente que ya ha ocurrido. A continuación, se presentan algunas brechas comunes que debe tener en cuenta:

- La telemetría enriquecida almacenada en los terminales o compartida con su conjunto de soluciones actual genera brechas de visibilidad que los equipos podrían pasar por alto.
- Reenviar algunos eventos (Windows) mientras se aíslan otros (Apple) en entornos multiplataforma sigue exponiendo a la organización a riesgos.
- Recopilar telemetría es solo una parte de la solución; debe revisarse regularmente y actuar en consecuencia para desbloquear su verdadero valor.

Por el contrario, los conjuntos de soluciones de seguridad maduros comparten las siguientes características constantes:

- La telemetría fluye de forma continua y está integrada en sus procesos, no se revisa solo cuando alguien se acuerda de hacerlo.
- Los datos recopilados se analizan frente a múltiples fuentes, se correlacionan y se priorizan según su gravedad. La clasificación manual puede hacer que se pasen por alto detalles críticos.
- Los equipos con programas de conformidad exitosos no son los más grandes ni los que tienen mayores presupuestos. Son los que aprovechan la telemetría que se genera antes de tomar decisiones o actuar.
- La visibilidad construida sobre los datos que ya tiene es, casi siempre, un camino más rápido que la visibilidad construida a partir de herramientas nuevas que no están integradas.

Conclusión

Vale la pena repetirlo: la telemetría, sin revisión, es solo un conjunto de datos almacenados en un archivo.

El flujo constante de datos con fecha y hora sobre lo que hace un dispositivo, su estado de configuración o su nivel de vulnerabilidad solo resulta útil cuando las organizaciones utilizan esta información para actuar sobre los hallazgos antes de que un problema menor se convierta silenciosamente en una infracción de conformidad costosa.

La capacidad de los datos de telemetría sin procesar para habilitar la toma de decisiones basada en datos, lo que conduce a acciones oportunas basadas en el estado en tiempo real, eso es la visibilidad. La precisión y la actualidad de los datos añaden una capa de confianza a la información que los acompaña a lo largo de su recorrido: desde el flujo de datos hasta quienes toman las decisiones en su destino final.

La brecha entre estar gestionado y estar protegido se puede cerrar. No siempre requiere nuevas compras, amplia experiencia a nivel de equipo ni cambios significativos en su conjunto de soluciones actual. Los dispositivos de su flota están diseñados para registrar lo que hacen, y ya le están contando todo lo que sucede.

La verdadera pregunta es si su organización está preparada para escuchar y actuar según lo que descubre.

¿Listo para verlo en acción?

Pruebe Jamf hoy mismo